The Mutually Unbiased Bases Revisited

Monique Combescure
IPNL, Bâtiment Paul Dirac
4 rue Enrico Fermi,Université Lyon-1
F.69622 VILLEURBANNE Cedex, France
email monique.combescure@ipnl.in2p3.fr

Abstract

The study of Mutually Unbiased Bases continues to be developed vigorously, and presents several challenges in the Quantum Information Theory.
Two orthonormal bases in $\mathbb{C}^d$, B and B' are said mutually unbiased if $\forall b \in B$, $b' \in B'$ the scalar product $b \cdot b'$ has modulus $d^{-1/2}$. In particular this property has been introduced in order to allow an optimization of the measurement-driven quantum evolution process of any state $\psi \in \mathbb{C}^d$ when measured in the mutually unbiased bases B_j of $\mathbb{C}^d$.
At present it is an open problem to find the maximal umber of mutually Unbiased Bases when d is not a power of a prime number.

In this article, we revisit the problem of finding Mutually Unbiased Bases (MUB's) in any dimension d. The method is very elementary, using the simple unitary matrices introduced by Schwinger in 1960, together with their diagonalizations. The Vandermonde matrix based on the d-th roots of unity plays a major role.
This allows us to show the existence of a set of 3 MUB's in any dimension, to give conditions for existence of more than 3 MUB's for d even or odd number, and to recover the known result of existence of $d+1$ MUB's for d a prime number. Furthermore the construction of these MUB's is very explicit.
As a by-product, we recover results about Gauss Sums, known in number theory, but which have apparently not been previously derived from MUB properties.

1 INTRODUCTION

Two orthonormal bases B and B' in $\mathbb{C}^d$ are called mutually unbiased if $|b \cdot b'| = d^{-1/2},\ \forall b \in B,\ b' \in B'$, where $v \cdot v'$ denotes the scalar product in $\mathbb{C}^d$. This notion first appeared in the literature in [12] in 1960, although the term "Mutually Unbiased Bases" (MUB) appeared later. It has attracted recently a great interest in the physics as well as mathematics literature, in conjunction with questions of Quantum Information, Quantum Cryptography, and Quantum Entanglement (see [4], [5], [7], [9], [10], [13], [14], and references therein contained). Note in particular that this property has been developed in order to allow an optimization of the measurement-driven quantum evolution process of any state $\psi \in \mathbb{C}^d$ when measured in the mutually unbiased bases B_j of $\mathbb{C}^d$ [11], [13].
If we denote by $N(d)$ the maximum cardinality of a set of MUB in $\mathbb{C}^d$, it has been established that

$$N(d) \leq d + 1$$

with equality for d being a power of a **prime number** (see [13], [7], [2], [9] and references herein contained).
In a number of previous works (see for example [1], [2], [4], [5], [8], [9], [10], [14]), it has been recognized that the construction of MUB's has to do with rather sophisticated arithmetical notions such as Weil sums over finite fields, Gauss Sums and Galois rings.
In this paper, we revisit these known results from an elementary point of view based on a simple set of $d \times d$ of unitary matrices. In [8], a recipe for an explicit constuction of the set of all MUB's for d a power of a prime has been provided, using the angular momentum bases. Strongly inspired by the recent work of Kibler and Planat [8], we reintroduce the matrices constructed by Schwinger, which allows us a construction of MUB's in different cases:
- d any integer
- d an odd integer
- d a prime number.

The three building block of unitary matrices that allow to perform our construction are, if $q := \exp(\frac{2i\pi}{d})$ the following:

$$U := \mathrm{diag}(1, q, q^2, ..., q^j, ..., q^{d-1})$$

$$V := \begin{pmatrix} 0 & 1 & 0 & . & . & 0 \\ 0 & 0 & 1 & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1 \\ 1 & 0 & 0 & . & . & 0 \end{pmatrix}$$

and for d an odd number

$$D := \mathrm{diag}(1, q, q^3, ...q^{\frac{j(j+1)}{2}}, ...1)$$

The result is that the diagonalization of the d matrices $V_k := VU^k,\ k \in \{0, 1, ..., d-1\}$ (also studied in [8]) provides us with a set of unitary matrices P_k which have certain "unbiasement" properties, according to the various cases listed above. A similar idea is also developped in [2] where the matrices U and V are called "generalized Pauli matrices on d-state quantum systems".
As a by-product, we recover certain properties of Gauss Sums, which to our knowledge has not been deduced from previous studies on MUB (see however the recent work [8] where a similar but different sum rule appears for d a prime number).

$$\left| \sum_{j=0}^{d-1} q^{\frac{kj(j+1)}{2}} \right| = \sqrt{d}, \text{ if } d \text{ is odd and } \forall k \text{ coprime with } d$$

This property can be found in the number theory literature ([3]).

2 THE SCHWINGER MATRICES

2.1 GENERAL DEFINITIONS AND PROPERTIES

In [12], two basic unitary $d \times d$ matrices $U,\ V$ are introduced. Let

$$q := \exp\left(\frac{2i\pi}{d}\right) \tag{2.1}$$

They are of the following form:

$$U := \mathrm{Diag}(1, q, q^2, ..., q^{d-1}) \tag{2.2}$$

$$V := \begin{pmatrix} 0 & 1 & 0 & . & . & 0 \\ 0 & 0 & 1 & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1 \\ 1 & 0 & 0 & . & . & 0 \end{pmatrix} \tag{2.3}$$

Lemma 2.1 *(i) $U,\ V$ obey the "q-commutation rule":*

$$VU = qUV \tag{2.4}$$

(ii) The Vandermonde matrix P_0 whose matrix elements for $j, k \in \{0, 1, ..., d-1\}$ are defined by

$$(P_0)_{j,k} := d^{-1/2} q^{jk} \tag{2.5}$$

is such that

$$V = P_0 U P_0^* \tag{2.6}$$

Definition 2.2 *For any $k \in \{0, 1, ..., d-1\}$ we define:*

$$V_k := VU^k = \begin{pmatrix} 0 & q^k & 0 & . & . & 0 \\ 0 & 0 & q^{2k} & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & q^{k(d-1)} \\ 1 & 0 & 0 & . & . & 0 \end{pmatrix} \tag{2.7}$$

Remark 2.3 *The matrices V_k have been first introduced in the study of MUB by Kibler-Planat [8].*

Definition 2.4 *(i) We say that a $d \times d$ unitary matrix A is "unbiased" is all its matrix elements $A_{j,k}$ sasisfy*

$$|A_{j,k}| = d^{-1/2}, \ \forall j, k \in \{0, 1, ..., d-1\} \tag{2.8}$$

(ii) We say that two $d \times d$ unitary matrices A, B are "mutually unbiased" if the matrix A^*B is unbiased.

Thus finding a MUB in dimension d amounts to exhibit a set that we call a MUM, of the following form:

$$\{\mathbb{1}_d, P_0, P_1, ..., P_m\} \tag{2.9}$$

(where $\mathbb{1}_d$ denotes the identity $d \times d$ matrix) such that $P_j, \ j \in \{0, 1, ..., m\}$ are "unbiased", and $P_j, \ P_k, \ j, k \in \{0, 1, ..., m\}, \ j \neq k$ are "mutually unbiased".

Proposition 2.5 *(i) Let , for any $k \in \{0, 1, ..., d-1\}$, P_k be a unitary $d \times d$ matrix, and D_k be the unitary diagonal matrix such that*

$$V_k = P_k D_k P_k^* \tag{2.10}$$

Then all matrices P_k are "unbiased matrices".
(ii) Furthermore $D_0 \equiv U$.

Lemma 2.6 *For any $k \in \{0, 1, ..., d-1\}$ one has*

$$U^k P_0 = P_0 (V^*)^k \tag{2.11}$$

Proof: It is known [3] (and easy to check) that $P_0^2 = W$ where $W \equiv W^*$ is the permutation matrix

$$W := \begin{pmatrix} 1 & 0 & 0 & 0 & . & . & 0 \\ 0 & 0 & 0 & 0 & . & . & 1 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 0 & 0 & 1 & 0 & . & . & 0 \\ 0 & 1 & 0 & 0 & . & . & 0 \end{pmatrix} \tag{2.12}$$

We want to prove that:

$$V^* = P_0^* U P_0$$

But using Lemma 2.2, this is equivalent to:

$$V^* = P_0^{*2} V P_0^2 \equiv WVW$$

which follows immediately from the property of the selfadjoint matrix W that:

$$WV^* = VW$$

Thus we have proven (2.11) for $k = 1$. The general statement follows by induction since:

$$U^k P_0 = UU^{k-1} P_0 = UP_0 (V^*)^{k-1} = P_0 (P_0^* U P_0)(V^*)^{k-1} = P_0 (V^*)^k \tag{2.13}$$

Proposition 2.7 *For* **any dimension** $d \geq 2$*, if* P_1 *be a unitary* $d \times d$ *matrix such that*

$$V_1 = P_1 D_1 P_1^*$$

then the matrices $P_1,\ P_0$ *are mutually unbiased* $d \times d$ *matrices.*

Proof: One has, using Lemma 2.1 (ii) and Lemma 2.6 for $k = 1$ that:

$$P_0^* V_1 P_0 = P_0^* V U P_0 = P_0^* V P_0 V^* = UV^*$$

Thus

$$P_0^* P_1 D_1 P_1^* P_0 = UV^*$$

which means that all column vectors of $P_0^* P_1$ are eigenstates of UV^* with eigenvalues being the diagonal elements of D_1 which are all of modulus 1. Since any eigenstate $v := (v_0, v_1, ..., v_{d-1})$ of the matrix UV^* satisfy $|v_j| = |v_j|,\ \forall j, k \in \{0, 1, ..., d-1\}$ and $P_0^* P_1$ is unitary, this implies the result.
□

Corollary 2.8 *For any integer* $d \geq 2$*, there is* **at least three MUB** *given by the bases defined by* $\mathbb{1}_d, P_0, P_1$*.*

The existence of at least 3 MUB's in any dimension is proven in [9].

2.2 THE EVEN CASE

Let d be **even**. Then the determinant of both U, V equals ± 1 depending on whether $d = 0$ or $2 \pmod 4$. Namely

$$\det U = q^{\frac{d(d-1)}{2}}$$

and $d(d-1)/2$ is half integer if $d = 2 \pmod 4$, and integer if $d = 0 \pmod 4$.
In both cases the matrix $V_1 = VU$ has thus determinant $+1$, which means that it is unitarily equivalent to ωU, where

$$\omega := \exp\left(\frac{i\pi}{d}\right)$$

The eigenstate $v^{(1)} := (1, a_1, a_2, ..., a_{d-1})$ of V_1 with eigenvalue ω is such that $a_1 = \omega^{-1} = a_{d-1}$, and obeys the recurrence relation

$$a_k = \omega^{1-2k} a_{k-1}$$

Thus solving he recurrence relation we have:

$$a_k = \omega^{\sum_{j=0}^{k}(1-2j)} = \omega^{k-k(k+1)} = \omega^{-k^2}$$

More generally the eigenstate $v^{(j)} := (1, b_1, ..., b_k, ..., b_{d-1})$ of V_1 with eigenvalue ω^{2j+1} is such that

$$b_k = \omega^{2jk-k^2} \equiv q^{jk}\omega^{-k^2}$$

This implies:

Proposition 2.9 *(i) The matrix P_1 defined by:*

$$P_1 = D' P_0$$

with

$$D' := \mathrm{diag}(1, \omega^{-1}, ..., \omega^{-k^2}, ..., \omega^{-1})$$

diagonalizes V_1, namely $D_1 \equiv \omega U$:

$$V_1 = \omega P_1 U P_1^*$$

(ii) The property already shown that P_0, P_1 are mutually unbiased reflects itself in the identity

$$|\mathrm{Tr} D'| = \left|\sum_{k=0}^{d-1} \omega^{k^2}\right| = \sqrt{d}$$

The proof of (i) is obvious. Furthermore (ii) results from a known property in number theory [3], that if d is even, then

$$\sum_{k=0}^{d-1} \exp\left(k^2 \frac{i\pi}{d}\right) = \sqrt{d} \exp\left(\frac{i\pi}{4}\right)$$

□

For d even but not **not a power of 2**, it is not known what is the maximum number of MUB's. For example for $d = 6$ there is a conjecture that $N(6) = 3$ (see Section 6 where an explicit set of 3 MUB's is constructed). For $d = 0 \pmod 4$, it is known that the "tensor-product method" provides sets of more than 3 MUB's (see [9]). In Section 7, we make explicit this construction of 4 (resp 5) MUB's in the case $d = 12$ (resp $d = 20$).

2.3 THE ODD CASE

Definition 2.10 *Let us define $F_d := \mathbb{Z}/d\mathbb{Z}$ which is the finite field of residues of n, $(mod\ d)$.*

Theorem 2.11 *Let $d \in \mathbb{N}$ be an* **odd** *number. Define the unitary diagonal matrix D as*

$$D := \mathrm{diag}(1, q, q^3, ...q^{\frac{j(j+1)}{2}}, ...1) \tag{2.14}$$

Then we have:
(i) The matrices V_k, $k \in F_d$ are all unitarily equivalent to U.
(ii) Let $P_k := D^{-k}P_0$; then, for all $k \in F_d$ one has:

$$P_k^* V_k P_k = U$$

In other words if $P_0 = (v_0, v_1, ..., v_{d-1})$, then

$$P_k^* = (v_0, q^k v_{d-1}, ..., q^{kj(j+1)/2} v_{d-j}, ..., v_1)$$

(iii) $\forall k \in F_d$, such that d, k are co-prime, one has

$$|\mathrm{Tr} D^k| = \sqrt{d} \tag{2.15}$$

Proof: (i) is a consequence of (ii). Let us prove (ii):
It is enough to check that

$$U = P_0^* D^k V U^k D^{-k} P_0$$

But U^k and D^{-k} being diagonal commute, so that we are left with

$$D^k V D^{-k} U^k = P_0 U P_0^*$$

this in turn is equivalent to

$$D^k V D^{-k} = V U^{-k} \equiv V_{-k}$$

or to the equation

$$D^k V = V_{-k} D^k$$

which follows easily from the fact that they are unitary matrices with only non-vanishing elements $a_{0,d-1} = 1$ and

$$a_{j,j+1} = \left(q^{\frac{k(k+1)}{2}}\right)^k, \ \forall j \in \{0, 1, ..., d-1\}$$

Now let us prove (iii). We need the following proposition:

Proposition 2.12 *Let $k \in F_d$, such that k, d are co-prime. Then the matrix $P_0^* P_k$ is unbiased.*

Proof: It follows from equ. (2.13) that

$$V_k P_0 \equiv V U^k P_0 = V P_0 (V^*)^k$$

and thus

$$P_0^* P_k U P_k^* P_0 = U (V^*)^k \tag{2.16}$$

(since by definition $V_k = P_k U P_k^*$)
But:

Lemma 2.13 *If d, $k \in F_d$ are co-prime, the matrix $(V^*)^k$ is a permutation matrix with cycle of length d, and thus all eigenstates of $U(V^*)^k$ have coordinates of equal modulus, namely $d^{-1/2}$,*

Proof: This is standard. For any d, $k \in F_d$ co-prime, there exists a cyclic permutation σ_k (that means a permutation with cycle of length d) of F_d such that for any $v \in \mathbb{C}^k$, the element $w \in \mathbb{C}^k$ defined by:

$$(V^*)^k v \equiv w$$

is such that

$$w_j = v_{\sigma_k(j)}, \ \forall j \in F_d$$

□

Remark 2.14 *The idea that the eigevectors of V_k are "cyclically shifted" modulo a phase if d is a prime number has already been put forward in [2].*

End of Pooof of Proposition 2.12:
Let us denote by $v^{(k)}$ the successive column vectors of $P_0^* P_k$. Then

$$P_0^* P_k U = (q^0 v^{(0)}, q v^{(1)}, ..., q^j v^{(j)}, ..., q^{d-1} v^{(d-1)})$$

This means that $v^{(j)}$ is eigenvector of the matrix $U(V^*)^k$ with eigenvalue q^j. Therefore we have that $|v_l^{(j)}| = |v_0^{(j)}|$, $\forall l \in \{0, 1, ..., d-1\}$, as a consequence of Lemma 2.13 above. Since $\|v\| = 1$, this implies $|v_k^{(j)}| = d^{-1/2}$. It follows that for all primes $k \in F_d$ that are relatively prime to d, one has that $P_k^* P_0$ is an unbiased matrix.
□

Proof of Theorem 2.11 (iii):
Let d, $k \in F_d$ be co-prime. Let us call v_k the normalized eigenvector of V_k with eigenvalue 1. We obviously have

$$(v_k)_j = \frac{1}{\sqrt{d}} \left(q^{\frac{j(j+1)}{2}} \right)^k$$

Now using that $P_0^* P_k$ is unbiased we have $|v_0 \cdot v_k| = d^{-1/2}$ and

$$v_0 \cdot v_k \equiv d^{-1} \sum_{j=0}^{d-1} (q^{\frac{j(j+1)}{2}})^k \equiv d^{-1} \mathrm{Tr}(D^k)$$

which yields the result. □

Corollary 2.15 *Let d be an* **odd number**. *Then for any $k \in F_d$ co-prime with d, we have:*

$$\left| \sum_{j=0}^{d-1} q^{\frac{kj(j+1)}{2}} \right| = \sqrt{d}$$

Remark 2.16 *Corollary 2.12 is strongly related to the property of Gauss Sums. In [3], the following result is established: define, for $a, b, d \in \mathbb{Z}$, with $ad+b$ even, and $ad \neq 0$*

$$S(a, b, d) := \sum_{n=0}^{d-1} \exp\left(\frac{i\pi(an^2 + bn)}{d} \right)$$

Then the following "reciprocity theorem for quadratic Gauss sums" yields that:

$$S(a, b, d) = \left| \frac{d}{a} \right| \exp\left(\frac{i\pi}{4} (sgn(ad) - b^2/ad) \right) S(-d, -b, a) \qquad (2.17)$$

Applying it with d **odd** *and $a = b = 1$, we have*

$$S(1, 1, d) = \sqrt{d} \exp\left(\frac{i\pi}{4} (1 - \frac{1}{d}) \right)$$

since $S(-d,1,1)=1$.
Thus arithmetics gives not only the modulus of $\mathrm{Tr}D$ *which equals* $\sqrt{d}$ *but also the phase. A similar result holds for* $\mathrm{Tr}D^k$ *provided* $d,\ k \in F_d$ *are co-prime.*

If d is not a prime number, and if the lowest common divisor of $d,\ k$ is 1, then the matrices $P_0,\ P_k$ have been shown to be mutually unbiased. In the **odd case**, when d is not a prime number, this appears very useful to find more than 3 MUB.

Proposition 2.17 *Let* d *be an odd integer. If* $E := \{k_j\} \subset \{0,1,...,d-1\}$ *is such that the lowest common divisor of* $d,\ k_j - k_{j'}$ *is 1 for all* $k_j,\ k_{j'} \in E$*, then the set*

$$\left\{\mathbb{1}_d, P_{k_j}\right\}_{k_j \in E}$$

defines a MUB.

Proof: The proof is quite simple and uses Theorem 2.11 (ii). Namely, since $P_k = D^{-k}P_0$, we have:

$$P_k^* P_j = P_0^* D^{k-j} P_0 = P_{k-j}^* P_0 \tag{2.18}$$

Now, this follows from Proposition 2.12.
□

Corollary 2.18 *Let* $d = mn,\ with\ n,m \in \mathbb{N}$ *prime numbers, and* $n < m$*. Then the cardinality of the set of* $d \times d$ *unbiaised bases* $N(d)$ *satisfies:*

$$N(d) \geq N(n) \equiv n+1$$

Proof: For n=2, we are in the **even case** studied in the previous subsection. It has already been established that $N(d) \geq 3$ (Corollary 2.8). If n is **odd**, (then so is m), the matrices P_k for $k \in F_n$ are all mutually unbiased. Thus we can choose as a MUM the set

$$\{\mathbb{1}_d, P_0, P_1, ..., P_{n-1}\}$$

□

Remark 2.19 *A similar, but apparently more general result, has been proven in [9].*

EXAMPLE 1: d=15 : There are 4 MUB's, defined either by

$\{\mathbb{1}_{15}, P_0, P_1, P_2\}$ $\{\mathbb{1}_{15}, P_0, P_2, P_4\}$ $\{\mathbb{1}_{15}, P_0, P_1, P_8\}$ $\{\mathbb{1}_{15}, P_0, P_4, P_8\}$ $\{\mathbb{1}_{15}, P_0, P_7, P_{14}\}$

EXAMPLE 2 : d=21 There are 4 MUB's, defined for example by

$$\{\mathbb{1}_{21}, P_0, P_1, P_2\}$$

Of course we do not know whether or not this is the maximum number of MUB's in these cases.

2.4 THE PRIME NUMBER CASE

Proposition 2.20 *Let us assume that d is a* **prime number**≥ 3. *Then all unitary* $d \times d$ *matrices* $P_0^* P_k,\ k \in \{0, 1, ..., d-1\}$ *are unbiased.*

Proof: Any prime number ≥ 3 being odd, the result is a consequence of Lemma 2.13, since then any $k \in F_d$ is relatively prime to d.
□

Theorem 2.21 *for d a* **prime number**, *the following set of matrices*

$$\left\{ \mathbb{1}_d, D^{-k} P_0,\ k = 0, 1, ..., d-1 \right\}$$

defines a maximal set of MUM.

Proof: We use Theorem 2.11: thus $P_k = D^{-k} U$, so that

$$P_k^* P_j = P_0^* D^{k-j} P_0 = P_{k-j}^* P_0$$

so that if $j \neq k$ the result follows from Proposition 2.12.
□

Remark 2.22 *The fact that in dimension d there is at most d+1 MUB, and exactly* $d+1$ *for d a prime number is known for a long time. See for example [14] and references herein contained.*

3 THE CASE WHERE d IS THE SQUARE OF A PRIME NUMBER

Consider the Tensor-Product $d^2 \times d^2$ matrices introduced by Kibler-Planat [8], (here restricted to two-tensor products):

$$W_{j,k} := V_j^{(d)} \otimes V_k^{(d)},\ j, k \in \{0, 1, ..., d-1\} \tag{3.1}$$

where d is a **prime number greater than or equal to 3**, and $V_j^{(d)}$ is the corresponding $d \times d$ matrices, for $j \in \{0, 1, ..., d-1\}$.
Let $U^{(d)} := \mathrm{diag}(1, q, ..., q^j, ..., q^{d-1})$ where q is defined by (2.1), and U be the $d^2 \times d^2$ diagonal unitary matrix

$$U := U^{(d)} \otimes U^{(d)}$$

Consider the unitary matrices $P_k^{(d)}$ constructed in the previous section, and let for $j, k \in \{0, 1, ..., d-1\}$ the $d^2 \times d^2$ unitary matrices

$$P_{j,k} := P_j^{(d)} \otimes P_k^{(d)}$$

Then we have:

Proposition 3.1

$$W_{j,k}P_{j,k} = P_{j,k}U$$

Proof: This immediately follows (omitting the superscript d for simplicity) from:

$$(V_j \otimes V_k)\ (P_j \otimes P_k) = (V_jP_j)\ \otimes\ (V_kP_k) = (P_jU)\ \otimes (P_kU) \equiv P_{j,k}U$$

□

Theorem 3.2 *(i) The matrices $P_{j,k}$ are unbiased $d^2 \times d^2$ matrices, $\forall j,k \in \{0,1,...,d-1\}$. (ii) For any $j,k \in \{0,1,...,d-1\}$, $k \neq j$, we have that $P_{j,j}$, $P_{k,k}$ are mutually unbiased $d^2 \times d^2$ matrices.*

Proof: Recall that the "tensor-product formalism" enables to write the $d^2 \times d^2$ matrices as 2×2 block forms of $d \times d$ matrives. Namely $\forall j,k \in F_d$,

$$W_{j,k} \equiv \begin{pmatrix} 0 & (-i)^j V_k \\ V_k & 0 \end{pmatrix} \quad P_{j,k} \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} P_k & P_k \\ i^j P_k & -i^j P_k \end{pmatrix} \quad U_{j,k} \equiv \begin{pmatrix} (-i)^j U_k & 0 \\ 0 & -(-i)^j U_k \end{pmatrix}$$

with U_k diagonal matrices such that

$$V_k = P_k U_k P_k^*$$

Then the result follows from Proposition 2.20.
□

Remark 3.3 *The above result provides only $d(d-1)/2$ MUB. But it is known (see [14], [8]) that the maximun number which is here d^2+1 is attained. There is a "trick", not explained here which allows to construct the "missing" bases, not only for the* **square of prime numbers**, *but more generally for* **any power of prime numbers.** *We shall give the explicit construction for $d = 4$ in Chapter 5.*

4 DIMENSIONS 2 AND 3

$$P_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad P_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$

Proposition 4.1 *(i) The sets*

$$E_2 := \{\mathbb{1}_2, P_0, P_1\}, \qquad E_2' := \{\mathbb{1}_2, P_1, P_1^*\}$$

are complete MUM in dimension d=2.
(ii) The bases in $\mathbb{C}^2$ defined by E_2 and E_2' are the same MUB in dimension d=2.

Proof: (i) results from Propositions 2.5 and 2.7, for E_2, and for E_2' from the fact that P_1^2 is unbiased (in other words P_1 is mutually unbiased to itself). Namely:

$$P_1^3 = e^{-i\pi/4}\mathbb{1}_2$$

which implies that $P_1^2 = e^{-i\pi/4}P_1^*$ which is unbiased.
(ii) Denote by $e_1 := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $e_2 := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ the natural basis in $\mathbb{C}^2$. Then the MUB defined by $E_2, \quad E_2'$ are $\{B_0, B_1, B_2\}$ where

$$B_0 := \{e_1, e_2\} \quad B_1 := \left\{\frac{1}{\sqrt{2}}(e_1 \pm e_2)\right\} \quad B_2 := \left\{\frac{1}{\sqrt{2}}(e_1 \pm ie_2)\right\}$$

□

For the case of dimension $d = 3$ we simply use Theorem 2.8 (ii) for the simple construction of $P_j,\ j \in \{0, 1, 2\}$:
Let $q = \exp(\frac{2i\pi}{3})$

$$P_0 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & q & q^2 \\ 1 & q^2 & q \end{pmatrix} \quad P_1 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ q^2 & 1 & q \\ 1 & q^2 & q \end{pmatrix} \quad P_2 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ q & q^2 & 1 \\ 1 & q^2 & q \end{pmatrix}$$

Proposition 4.2 *(i) The set $E_3 := \{\mathbb{1}_3, P_0, P_1, P_2\}$ defines a maximal MUM for d=3.*
(ii) Define:

$$P_1' := \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & q \\ 1 & q & 1 \\ q & 1 & 1 \end{pmatrix}$$

Then the set $E_3' := \left\{\mathbb{1}_3, P_0, P_1', P_1'^*\right\}$ defines a maximal MUM in dimension d=3.

Proof: (i) simply follows from Theorem 2.14. Furthermore E_3' defines the same MUB as E_3, which establishes (ii).
□

5 THE CASE OF DIMENSION 4

There is nothing new in the results of this section (see [2], [8], [14]). The only point is that we construct explicit matrices that allow to complete the set of MUM provided in Section 3.
According to Theorem 3.2, we have that $P_{0,0},\ P_{1,1}$ are mutually unbiased matrices. However $P_{0,1},\ P_{1,0}$ are not mutually unbiased, neither to each other, nor to the two previous ones. TThe trick is to consider that the eigenspaces of $W_{0,1},\ W_{1,0}$ with

eigenvalues $\pm i$ are degenerate, so that vectors of these eigenspaces can be recombined to build MUB's.
Namely take

$$P'_{0,1} := \frac{1}{\sqrt{2}} \begin{pmatrix} P_0 & P_0 \\ -iP'_0 & iP'_0 \end{pmatrix} \quad P'_{1,0} := \frac{1}{\sqrt{2}} \begin{pmatrix} P_1 & P_1 \\ -P'_1 & P'_1 \end{pmatrix} \quad P'_{0,0} \equiv P_{0,0} \quad P'_{1,1} \equiv P_{1,1}$$

with

$$P'_0 := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad P'_1 := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}$$

Actually, defining the unitary 4×4 matrix (that commutes with $U_{1,0}$ and $U_{0,1}$) as

$$A := \frac{e^{-i\pi/4}}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & i \\ 0 & 1 & i & 0 \\ 0 & i & 1 & 0 \\ i & 0 & 0 & 1 \end{pmatrix}$$

we have:

$$P_{1,0} = P'_{1,0}A \qquad P_{0,1} = P'_{0,1}A^*$$

Then

Proposition 5.1

$$W_{0,1}P'_{0,1} = P'_{0,1}U_{0,1}, \quad W_{1,0}P'_{1,0} = P'_{1,0}U_{1,0}$$

and $P'^*_{i,j}P'_{k,l}$ *are unbiased matrices* $\forall (i,j) \neq (k,l)$ $i,j,k,l \in \{0,1\}$.

Proof: We check that $P'^*_{0,1}P_{1,0}$ is an unbiased matrix. We have:

$$P'^*_{0,1}P_{1,0} = \frac{1}{2} \begin{pmatrix} (P_0^* - iP_0'^*)P_1 & (P_0^* + iP_0'^*)P_1 \\ (P_0^* + iP_0'^*)P_1 & (P_0^* - iP_0'^*)P_1 \end{pmatrix}$$

But

$$(P_0^* - iP_0'^*)P_1 = \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \qquad (P_0^* + iP_0'^*)P_1 = \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}$$

The other cases can be shown similarly.
□

6 THE CASE OF DIMENSION 6

It is le least even dimension which in not **the power of a prime number**. Let $j := \exp(\frac{2i\pi}{6})$. Then

$$P_0 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & j & j^2 & -1 & -j & -j^2 \\ 1 & j^2 & -j & 1 & j^2 & -j \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -j & j^2 & 1 & -j & j^2 \\ 1 & -j^2 & -j & -1 & j^2 & j \end{pmatrix} \quad P_1 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ -ij^2 & i & ij & ij^2 & -i & -ij \\ 1 & j^2 & -j & 1 & j^2 & -j \\ -i & i & -i & i & -i & i \\ j^2 & 1 & -j & j^2 & 1 & -j \\ -i & ij^2 & ij & i & -ij^2 & -ij \end{pmatrix}$$

Lemma 6.1 *Let $\tilde{D}$ be the following unitary diagonal matrix:*

$$\tilde{D} := \mathrm{diag}(1, -ij^2, 1, -i, j^2, -i)$$

Then we have:

$$P_1 = \tilde{D} P_0$$

Proposition 6.2 *The set $E_6 := \{\mathbb{1}_6, P_0, P_1\}$ defines a MUM in dimension d=6.*

Proof: This follows simply from Ptoposition 2.5 and Proposition 2.7. Moreover we have:

$$P_0^* V P_0 = U \qquad P_1^* V_1 P_1 = iU$$

□

Remark 6.3 *The fact that $N(6) = 3$ is the maximum number of MUB in dimension 6 is a conjecture apparently due to Zauner [15]. Some progress has been recently made in dimension 6 by M. Grassl [6].*

7 THE CASE OF DIMENSIONS 12 AND 20

Let $d = 4m$ where m is an odd number ≥ 3. Then consider the 4×4 matrices $W_k,\ k = 0, 1, ..., 3$ constructed in Section 3, together with the set of matrices $V_k,\ k \in F_m$ constructed in Subsection 2.3. Denote by $Q_j,\ j = 0, 1, ..., 3$ the unitary 4×4 matrices $P_{k,l},\ k, l \in \{0, 1\}$, (in lexicographic order) provided in Section 5 for $d = 4$, and by $P_j,\ j \in F_m$ the $m \times m$ unitary matrices constructed in Subsection 2.3. Then one has:

Lemma 7.1 *For any $j = 0, 1, ..., \mathrm{Inf}(4, m+1)$, there exists a* **diagonal matrix** *U_j such that*

$$(W_j \otimes V_j)\ (Q_j \otimes P_j) = (Q_j \otimes P_j) U_j$$

The proof is very similar to the one provided in Section 3. Furthemore the idea of tensor-product methods in this situation is already present in [9].

Actually the new ingredient in this Section is to establish explicit $4m \times 4m$ matrices $R_j := Q_j \otimes P_j$ in $4times4$ or $m \times m$ block forms; let us specify them for $m = 3,\ m = 5$:

Lemma 7.2 *(i) Let $d = 12$. Thus $m = 3$ and denoting by q the 3rd root of unity $q := \exp(2i\pi/3)$, we have:*

$$R_0 := \frac{1}{\sqrt{3}} \begin{pmatrix} Q_0 & Q_0 & Q_0 \\ Q_0 & qQ_0 & q^2Q_0 \\ Q_0 & q^2Q_0 & qQ_0 \end{pmatrix} \quad R_1 := \frac{1}{\sqrt{3}} \begin{pmatrix} Q_1 & Q_1 & Q_1 \\ q^2Q_1 & Q_1 & qQ_1 \\ Q_1 & q^2Q_1 & qQ_1 \end{pmatrix}$$

$$R_2 := \frac{1}{\sqrt{3}} \begin{pmatrix} Q_2 & Q_2 & Q_2 \\ qQ_2 & q^2Q_2 & Q_2 \\ Q_2 & q^2Q_2 & qQ_2 \end{pmatrix}$$

The matrices $R_j,\ j = 0, 1, 2$ are obviously unbiased unitary matrices and are mutually unbiased. Thus the set $\{\mathbb{1}_{12}, R_0, R_1, R_2\}$ defines a set of 4 MUB's for $d = 12$. Futhermore any choice of Q_j's among the 4 matrices $P_{j,k}, j, k \in \{0, 1\}$ (not necessarily the lexicographic order) gives the same result, but not the same MUB's.

(ii) Let $d = 20$, thus $m = 5$. Take 4 unitary 5×5 matrices among the 6 possible P_j's in dimension 5. Then we have:

$$R'_0 := \frac{1}{2} \begin{pmatrix} P_0 & P_0 & P_0 & P_0 \\ P_0 & -P_0 & P_0 & -P_0 \\ P_0 & P_0 & -P_0 & -P_0 \\ P_0 & -P_0 & -P_0 & P_0 \end{pmatrix} \quad R'_1 := \frac{1}{2} \begin{pmatrix} P_1 & P_1 & P_1 & P_1 \\ P_1 & -P_1 & P_1 & -P_1 \\ -iP_1 & -iP_1 & iP_1 & iP_1 \\ iP_1 & -iP_1 & -iP_1 & iP_1 \end{pmatrix}$$

$$R'_2 := \frac{1}{2} \begin{pmatrix} P_2 & P_2 & P_2 & P_2 \\ iP_2 & -iP_2 & iP_2 & -iP_2 \\ -P_2 & -P_2 & P_2 & P_2 \\ iP_2 & -iP_2 & -iP_2 & iP_2 \end{pmatrix} \quad R'_3 := \frac{1}{2} \begin{pmatrix} P_3 & P_3 & P_3 & P_3 \\ iP_3 & -iP_3 & iP_3 & -iP_3 \\ iP_3 & iP_3 & -iP_3 & -iP_3 \\ -P_3 & P_3 & P_3 & -P_3 \end{pmatrix}$$

Then the 20×20 unitary matrices $R'_j,\ j = 0, 1, ...3$ are unbiaised and mutually unbiased. Thus the set

$$\{\mathbb{1}_{20}, R'_0, R'_1, R'_2, R'_3\}$$

defines a set of 5 MUB's.

Acknowledgements : It is a pleasure to thank M. Kibler for learning me everything about MUB's, providing me with [8] before publication and for his careful reading of this manuscript. I am also indebted to F. Moulin and J. Marklof for useful informations and comments about Gauss Sums.

References

[1] Archer C., *There is no generalization of known formulas for mutually unbiased bases*, J. Math. Phys., **46** 022106, (2005)

[2] Bandyopadhyay S., Boykin P.O., Roychowdhury V., Vatan F., *A new proof of the existence of mutually unbiased bases*, Algorithmica, **34**, 512-528, (2002)

[3] Berndt B.C., Evans R.J., Williams K.S., *Gauss and Jacobi Sums*, Canadian Mathematical Society, Vol **21**, Wiley-Interscience Publication

[4] Chaturvedi S., *Mutually unbiased bases*, Pramana J. of Phys., **59**, 345-350, (2002)

[5] Chaturvedi S., *Aspects of mutually unbiased bases in odd prime dimensions*, Phys. Rev. A **65**, 044301 (2002)

[6] Grassl M., *On SIC-POVMs and MUBs in dimension 6*, arXiv:quant-ph/ 0406175, (2004)

[7] Ivanović I.D., *Geometrical description of quantal state determination*, J. Phys. A, Mathem. and General, **14**, 3241-3245, (1981)

[8] Kibler M., Planat M., *A $SU(2)$ recipe for mutually unbiased matrices* arXiv:quant-ph/0601092 (2006)

[9] Klappenecker A., Rötteler M., *Constructions of Mutually Unbiased Bases*, arXiv:quant-ph/0309120, (2003)

[10] Planat M., Rosu H., *Mutually unbiased phase states, phase uncertainties, and Gauss sums*, Eur Phys. J. D **36**, 133-139, (2005)

[11] Roa L., Delgado A., Ladron de Guevara M. L., Klimov A. B., *Measurement-driven quantum evolution*, Phys. Rev. A, **73**, 012322, (2006)

[12] Schwinger J., *Unitary Operator Bases*, Proc Nat. Acad. Sci. U.S.A. **46**, 560 (1960)

[13] Wootters W.K., Fields B.D., *Optimal state-determination by mutually unbiased measurements*, Ann. Phys., **191**, 363-381, (1989)

[14] Wootters W.K., *Quantum Measurements and Finite Geometry*, Foundations of Physics, (to appear)

[15] Zauner G., *Quantendesigns- Grundzüge einer nichtkommutativen Designtheorie*, PhD Thesis, Universität Wien (1999)